

REMARKS

In response to the Office Action dated July 28, 2004, Applicant respectfully requests reconsideration and withdrawal of the rejection of the claims.

Claims 1-13 were rejected under 35 U.S.C. §102, on the grounds that they were considered to be anticipated by the *Rothermel et al.* patent (U.S. 6,678,827). It is respectfully submitted that the *Rothermel et al.* patent neither anticipates, nor otherwise suggests, the claimed subject matter.

Claim 1 recites a method for automatically provisioning a plurality of computing devices in accordance with established policies. The claimed method comprises three steps, namely creating a plurality of templates reflecting the policies, expanding at least one template at a central location, and providing the expanded information to the plurality of computer devices. In connection with this subject matter, the Office Action refers to the *Rothermel et al.* patent at column 4, line 49, through column 5, line 13. This portion of the patent generally describes the use of templates to implement security policies. However, it does not disclose the steps of *expanding* at least one template at a central location, and providing *the expanded information* to a plurality of computing devices.

In the disclosed embodiment of the invention, the expansion of a template involves the creation of a document, such as an XML document, that contains a list of not only those users who are explicitly identified within the template, but also those users who are identified in information that is external to the template, and referenced therein. For instance, the application discloses an example in which a reference is made to an external list of database administrators. By utilizing such an approach, it is only necessary to maintain a single list of database administrators.

Each time an updated security policy is to be provided to a device, this single external list is referenced and used to create the information within the expanded XML document. Thus, each time a database administrator is added or removed, it is not necessary to edit every template that pertains to a database server. Rather, only the external list needs to be kept up to date.

It is respectfully submitted that the *Rothermel et al.* patent does not disclose the concept of *expanding* a template, for example by including information from a source of information external to the template, and providing this expanded information to a computing device.

Another feature of the invention that is recited, for example, in claims 3 and 9, is the ability to include conditional statements in a template. This ability greatly contributes to the flexibility of the present invention, by enabling additional policy information to be included within a template, but to be supplied to a given device only if that device meets the condition. This avoids the need to create a different template for every different type of device.

In rejecting claim 3, the Office Action refers to the *Rothermel et al.* patent at column 4, lines 30-62, and column 5, lines 60-67. It is not seen where either of these portions of the reference discloses, or otherwise suggests, the use of a conditional statement in a security policy template. If the rejection of claim 3 is not withdrawn, the Examiner is requested to explain how these portions of the reference are being interpreted to anticipate the use of conditional statements in security policy templates.

Another distinguishing feature of the invention resides in the fact that it is directed to user accounts that determine those persons who are authorized to

access networked computing devices, such as servers. Amended claims 7 and 13, as well as new claims 22-32, bring out this aspect of the invention. In contrast, the *Rothermel et al.* patent is directed to network security devices (NSDs), such as firewalls and the like. See, for example, column 1, line 26, and column 6, lines 15-16. In the case of the present invention, the security policy that is provided to a given device determines who has the right to access *that* device. In contrast, a network security device such as a firewall is designed to sit between a trusted device and an external device. The security policy that is provided to the NSD determines which external devices can gain access to a trusted device, rather than which users can access the NSD.


Claims 4-6 and 10-12 pertain to another feature of the invention, in which the templates are classified into multiple categories. One or more of the templates is global in nature, and applies to all of the computing devices under consideration, whereas others of the templates apply to only a subset of the computing devices, or only individual ones of the computing devices. In rejecting each of these claims, the Office Action refers to the *Rothermel et al.* patent at column 6, lines 20-32. This portion of the patent refers to different classes of *devices*, which have different security policies defined for each. It does not disclose, nor otherwise suggest, different categories of *templates* having different scopes of applicability, as recited in the claims.

In view of the foregoing, it is respectfully submitted that the claimed subject matter is not anticipated by the *Rothermel et al.* patent. Reconsideration and withdrawal of the rejection, and allowance of all pending claims are respectfully requested.

Respectfully submitted,

BURNS, DOANE, SWECKER & MATHIS, L.L.P.

Date: January 28, 2005

By: 
James A. LaBarre
Registration No. 28,632

P.O. Box 1404
Alexandria, Virginia 22313-1404
(703) 836-6620